US-CERT National Cyber Alert System

SB04-259-Summary of Security Items from September 8 through September 14, 2004

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans identified between September 7 and September 14, 2004. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Adobe Systems Adobe Acrobat 5.0.5 and prior, possibly 6.0.2	A buffer overflow vulnerability exists in Acrobat/Acrobat Reader due to a boundary error within the "pdf.ocx" ActiveX component supplied with Adobe Acrobat Reader. A remote malicious user can exploit this vulnerability via a malicious website using a specially crafted URL to potentially execute arbitrary code. Successful exploitation allows remote malicious users to utilize the arbitrary word overwrite to redirect the flow of control and eventually take control of the affected system. Code execution will occur under the context of the user that instantiated the vulnerable version of Adobe Acrobat. **Patch available at:** **http://www.adobe.com/support/downloads/thankyou.jsp?ftpID=2589&fileID=2433** Vendor asserts this vulnerability is fixed in version 6.0.2. However, proof of concept code exists that causes a Denial of Service.	Adobe Acrobat/Acrobat Reader ActiveX Control Buffer Overflow Vulnerability CVE Name: CAN-2004-0629	High	iDEFENSE Security Advisory 08.13.04 **SecurityFocus, September 8, 2004**
Cerulean Studios Trillian 0.74i	A buffer overflow vulnerability exists due to a boundary error in the MSN module, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published.	Trillian Remote Buffer Overflow MSN Module	High	Secunia Advisory, SA12487, September 8, 2004
F-Secure Anti-Virus for MS Exchange 6.0 1, 6.2, 6.21, Content Scanner Server 6.31, Internet Gatekeeper 6.3-6.32	A remote Denial of Service vulnerability exists due to an input validation error in F-Secure's Internet Gatekeeper. Hotfix available at: http://www.f-secure.com/security/fsc-2004-2.shtml We are not aware of any exploits for this vulnerability.	F-Secure Content Scanner Server Remote Denial of Service CVE Name: CAN-2004-0830	Low	iDEFENSE Security Advisory, September 9, 2004
gadu-gadu.pl Gadu-Gadu 6.0 build 149	A buffer overflow vulnerability exists due to a boundary error in the schema for sending images, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Gadu-Gadu Remote Buffer Overflow	High	Sec-Labs Team Advisory, September 12, 2004
getSolutions getIntranet 2.2	Multiple input validation vulnerabilities exist in the 'welcome.asp,' 'checklogin.asp,' and 'lostpassword.asp' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code, obtain sensitive information, or obtain elevated privileges. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	GetIntranet Multiple Remote Input Validation	Medium/ High (High if arbitrary code can be executed)	CRIOLABS Security Advisory, September 9, 2004
Jigunet Corporation Twin FTP Server 1.x	A Directory Traversal vulnerability exists due to an input validation error when processing arguments passed via the 'CWD,' 'STOR,' and 'RETR' FTP commands. Upgrade to Version 1.0.3 R3 that is released on 10 Sep 2004. Version 1.0.3 R3 released before 10 Sep 2004 is vulnerable. http://www.twinftp.com/index_kr.html?mod=down We are not aware of any exploits for this vulnerability.	TwinFTP Server Directory Traversal	Medium	SIG^2 Vulnerability Research Advisory, September 12, 2004
MailEnable Pty. Ltd. MailEnable 1.8, 1.71, 1.72, Professional 1.2 a, 1.2, 1.18, 1.19	A remote Denial of Service vulnerability exists due to an error when processing DNS responses. Hotfix available at: http://www.mailenable.com/hotfix/MEW2KDNS.zip There is no exploit code required.	MailEnable DNS Remote Denial of Service	Low	SecurityTracker Alert ID, 1011198, September 9, 2004
Microsoft Microsoft Office 2000 SP3, Word 2000, FrontPage 2000, Publisher 2000, Office XP SP3,Word 2002, FrontPage 2002, Publisher 2002, Office 2003, Word 2003, FrontPage 2003, Publisher 2003, Microsoft Works Suites, Works Suite 2001, 2002, 2003, 2004,	A buffer overflow vulnerability exists in the WordPerfect 5.x converter, which could let a remote malicious user execute arbitrary code. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms04-027.mspx We are not aware of any exploits for this vulnerability.	Microsoft Office WordPerfect Converter Buffer Overflow CVE Name: CAN-2004-0573	High	Microsoft Security Bulletin, MS04-027, September 14, 2004
Microsoft Microsoft .NET Framework 1.x, Digital Image Pro 7.x, 9.x, Digital Image Suite 9.x, Frontpage 2002, Greetings 2002, Internet Explorer 6, Office 2003 Professional Edition, 2003 Small Business Edition, 2003 Standard Edition, 2003 Student and Teacher Edition, Office XP, Outlook 2002, 2003, Picture It! 2002, 7.x, 9.x, PowerPoint 2002, Producer for Microsoft Office PowerPoint 2003, Project 2002, 2003, Publisher 2002, Visio 2002, 2003, Visual Studio .NET 2002, 2003, Word 2002	A buffer overflow vulnerability exists in the processing of JPEG image formats, which could let a remote malicious user execute arbitrary code. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx We are not aware of any exploits for this vulnerability.	Microsoft JPEG Processing Buffer Overflow CVE Name: CAN-2004-0200	High	Microsoft Security Bulletin, MS04-028, September 14, 2004 US-CERT Vulnerability Note VU#297462, September 14, 2004
Microsoft Internet Explorer 5.5, SP1&SP2. 6.0, SP1	A vulnerability exists due to insufficient validation of drag and drop events issued from the 'Internet' zone, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proof of Concept exploit has been published. **Functional exploit code is publicly available, and there are reports of incidents such as Akak that involve these vulnerabilities.**	Internet Explorer Drag & Drop File Installation CVE Name: CAN-2004-0839	High	Secunia Advisory, SA12321 August 19, 2004 **Vulnerability Note VU#526089, September 14, 2004**
RhinoSoft.com Serv-U 3.0, 3.1, 4.0 .0.4, 4.1 .0.11, 4.1, 4.2, 5.0 .0.9, 5.0 .0.6, 5.0.0.4, 5.1 .0, 5.2 .0.0	A remote Denial of Service vulnerability exists due to insufficient validation of arguments passed via the 'STOU' command. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit has been published.	Serv-U FTP Server Remote Denial of Service	Low	Bugtraq, September 11, 2004
SapporoWorks BlackJumboDog FTP Server 3.6.1	A buffer overflow vulnerability exists in which a remote malicious user can execute arbitrary code on the target system. A remote user can send a specially crafted FTP command with a long parameter string to trigger the flaw. The USER, PASS, RETR, CWD, XMKD, XRMD, and other commands are affected. The software reportedly copies the user-supplied parameter string to a 256 byte buffer. Update to version 3.6.2, available at: http://homepage2.nifty.com/spw/software/bjd/	BlackJumboDog Has Buffer Overflow in the FTP Service	High	US-CERT VU#714584, August 3, 2004 SecuriTeam, August 4, 2004 **SecurityFocus,**

	An exploit script has been published.			**September 10, 2004**
South River Technologies Titan FTP Server 2.2, 2.10, 3.0 1, 3.10, 3.21	A heap overflow vulnerability exists in the 'cwd' command due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code. **Upgrade available at: http://www.titanftp.com/products/titanftp/relnotes.html** Proof of Concept exploit script has been published.	Titan FTP Server CWD Command Remote Heap Overflow	High	www.cnhonker.com Security Advisory, August 29, 2004 **SecurityFocus, September 9, 2004**
TYPSoft TYPSoft FTP Server 0.85, 0.93, 0.95-0.97, 0.97.5, 0.99.6, 1.0-1.0 9, 1.1, 1.10, 1.11	A remote Denial of Service vulnerability exists when an authenticated malicious user (including an anonymous user) issues two consecutive 'RETR' commands followed by a 'QUIT' command. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	TYPSoft FTP Server Remote 'RETR' Denial of Service	Low	SecurityFocus, September 7, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Apache Software Foundation Apache 2.0.50	A remote Denial of Service vulnerability exists in 'char_buffer_read()' when using a RewriteRule to reverse proxy SSL connections. Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126 SuSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required; however, Proofs of Concept exploits have been published.	Apache mod_ssl Remote Denial of Service CVE Name: CAN-2004-0751	Low	SecurityTracker Alert ID, 1011213, September 10, 2004
Adobe Systems Adobe Acrobat Reader 5.05 and 5.06	An input validation and boundary error vulnerability exists in the uudecoding feature of Adobe Acrobat Reader, which can be exploited by a malicious user to compromise a user's system. The input validation error allows the injection of arbitrary shell commands. The boundary vulnerability can be exploited to cause a buffer overflow via a malicious PDF document with an overly long filename. Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into opening a malicious document. Update to version 5.09 for UNIX available at: http://www.adobe.com/products/acrobat/readstep2.html **Gentoo: http://security.gentoo.org/glsa/glsa-200408-14.xml** **RedHat: http://rhn.redhat.com/errata/RHSA-2004-432.html** **SuSE: ftp://ftp.suse.com/pub/suse/** We are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader Shell Command Injection & Buffer Overflow Vulnerability CVE Names: CAN-2004-0630 CAN-2004-0631	High	Secunia, SA12285, August 13, 2004 iDEFENSE Advisories 08.12.04 **Gentoo Linux Security Advisory GLSA 200408-14, August 15, 2004** **RedHat Security Advisory, RHSA-2004:432-08, August 31, 2004** **SUSE Security Announcement, SA:2004:028, September 1, 2004**
Apple Mac OS X 10.2.8, 10.3.4, 10.3.5	A remote Denial of Service vulnerability exists in the QuickTime Streaming Server when a malicious user submits a particular sequence of operations. Security update available at: http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	Apple QuickTime Streaming Server Remote Denial of Service CVE Name: CAN-2004-0825	Low	APPLE-SA-0024-09-07 Security Update, September 7, 2004
Apple Mac OS X 10.2.8, 10.3.4, 10.3.5	A vulnerability exists in Apple Safari due to the way frames are processed, which could let a remote malicious user execute arbitrary HTML code. Security update available at: http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	Apple Safari Frame Remote Arbitrary Code Execution CVE Name: CAN-2004-0720	High	APPLE-SA-0024-09-07 Security Update, September 7, 2004
Apple Mac OS X 10.2.8, 10.3.4, 10.3.5	A vulnerability exists in the PPPDialer because log files are stored in a world-writeable location, which could let a malicious user obtain elevated privileges. Security update available at: http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	PPPDialer Unsafe Log Files Elevated Privileges CVE Name: CAN-2004-0824	Medium	APPLE-SA-0024-09-07 Security Update, September 7, 2004
BEA Systems WebLogic Server & Express 6.1 SP6, 7.0 SP5, and 8.1 SP2; and prior service packs	A vulnerability exists in the Administrative Console because in some situations the password is echoed back to the administrator when booting the server, which could let a malicious user obtain sensitive information. Fixes available at: dev2dev.bea.com/resource library/advisoriesnotifications/BEA04-69.00.jsp We are not aware of any exploits for this vulnerability	WebLogic Administrative Console Password Disclosure	Medium	BEA Security Advisory, BEA04-69.00, September 13, 2004
Caolan McNamara and Dom Lachowicz wvWare version 0.7.4, 0.7.5, 0.7.6 and 1.0.0	A buffer overflow vulnerability exists due to the insecure function call strcat() without appropriate bounds checking, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.abisource.com/bonsai/cvsview2.cgi?diff_mode=context&whitespace_mode=show&root=/cvsroot&subdir=wv&command=DIFF_FRAMESET&root=/cvsroot&file=field.c&rev1=1.19&rev2=1.20 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200407-11.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva: ftp://atualizacoes.conectiva.com.br/** A Proof of Concept exploit has been published.	wvWare Library Buffer Overflow Vulnerability CVE Name: CAN-2004-0645	High	Securiteam, July 11, 2004 iDEFENSE Security Advisory, July 9, 2004 **Conectiva Linux Security Announcement, CLA-2004:863, September 10, 2004**
Ethereal Ethereal 0.x	Multiple Denial of Service and buffer overflow vulnerabilities exist due to errors in the iSNS, SNMP, and SMB dissectors which may allow an attacker to run arbitrary code or crash the program. Updates available at:http://www.ethereal.com/download.html or disable the affected protocol dissectors. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Debian: http://lists.debian.org/debian-security-announce/debian- security-announce-2004/msg00129.html An exploit script has been published.	Ethereal: Multiple security problems CVE Names: CAN-2004-0633, CAN-2004-0634, CAN-2004-0635	Low/High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200407-08 / Ethereal, July 9, 2004 Secunia Advisory, 12034 & 12035, July 12, 2004 Ethereal Advisory, enpa-sa-00015, July 6, 2004

				US-CERT Vulnerability Notes VU#518782, VU#829422, VU#835846, September 7, 2004
Gnome Multi Terminal Gnome Multi Terminal 1.6.2-r1	A vulnerability exists in the '.xsession-errors' file, which could let a malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200409-10.xml There is no exploit code required.	Multi Gnome Terminal Information Leak	Medium	Gentoo Linux Security Advisory, GLSA 200409-10, September 6, 2004
GNU gnubiff 1.0.1-1.0.10, 1.2, 1.4	Two vulnerabilities exist: a remote Denial of Service vulnerability exists in the POP3 functionality; and a remote Denial of Service vulnerability exists in the POP3 functionality when processing UIDL lists. The execution of arbitrary code may also be possible. Upgrades available at: http://prdownloads.sourceforge.net/gnubiff/gnubiff-2.0.1.tar.gz?download We are not aware of any exploits for this vulnerability.	gnubiff Multiple Remote POP3 Protocol Vulnerabilities	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA12445, September 6, 2004
J.Schilling Star Tape Archiver 1.5a09-1.5a45	A vulnerability exists in the setuid function due to a failure to properly implement the function when ssh is used for remote tape access, which could let a malicious user obtain superuser access. Update available at: http://ftp.berlios.de/pub/schily/star/alpha/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-11.xml We are not aware of any exploits for this vulnerability.	Star Tape Archiver Superuser Access	High	SecurityTracker Alert ID: 1011195, September 8, 2004
Jamie Cameron Usermin 1.0 80, 1.0 70, 1.0 60, 1.0 51, 1.0 40, 1.0 30, 1.0 20, 1.0 10, 1.0 00, Webmin1.0 90, 1.0 80, 1.0 70, 1.0 60, 1.0 50, 1.0 20, 1.0 00, 1.100, 1.110, 1.121, 1.130, 1.140, 1.150	A vulnerability exists due to the insecure creation of temporary files during installation, which could let a malicious user obtain sensitive information. Usermin: http://freshmeat.net/redir/usermin/28573/url_tgz/usermin-1.090.tar.gz Webmin: http://prdownloads.sourceforge.net/webadmin/webmin-1.160.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-15.xml There is no exploit code required.	Webmin / Usermin Insecure Temporary File CVE Name: CAN-2004-0559	Medium	SecurityFocus, September 10, 2004
John Sterling mod_cplusplus 1.1 .0, 1.2, 1.3, 1.3.1, 1.4 .0	A buffer overflow vulnerability exists which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/modcplusplus/mod_cplusplus-1.4.1.tar.gz?download We are not aware of any exploits for this vulnerability.	Mod_cplusplus Buffer Overflow	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 10, 2004
MIT Debian Fedora Gentoo Immunix Mandrake OpenBSD RedHat SGI Sun Tinysofa Trustix Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2.1-1.2.7, 1.3 -alpha1, 5.0 -1.3.3, 5.0 -1.2beta1&2, 5.0 -1.1.1, 5.0 -1.1, 5.0 -1.0.x; tinysofa enterprise server 1.0 -U1, 1.0	Multiple buffer overflow vulnerabilities exist due to boundary errors in the 'krb5_aname_to_localname()' library function during conversion of Kerberos principal names into local account names, which could let a remote malicious user execute arbitrary code with root privileges. Patch available at: http://web.mit.edu/kerberos/advisories/2004-001-an_to_ln_patch.txt Mandrake: http://www.mandrakesoft.com/security/advisories Tinysofa: http://www.tinysofa.org/support/errata/2004/009.html Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/k/krb5/ Fedora: http://securityfocus.com/advisories/6817 RedHat: http://rhn.redhat.com/errata/RHSA-2004-236.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ Sun: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57580 Gentoo: http://security.gentoo.org/glsa/glsa-200406-21.xml **Apple: http://www.apple.com/support/downloads/** Currently we are not aware of any exploits for this vulnerability.	Kerberos 5 'krb5_aname_to_localname' Multiple Buffer Overflows CVE Name: CAN-2004-0523	High	MIT krb5 Security Advisory 2004-001, June 3, 2004 TA04-147A, http://www.kb.cert.org/vuls/id/686862tp **Apple Security Update, APPLE-SA-2004-09-07, September 7, 2004**
Mr. S.K. LHA 1.14	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the parsing of archives, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the parsing of command-line arguments, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to insufficient validation of shell meta characters in directories, which could let a remote malicious user execute arbitrary shell commands. RedHat: http://rhn.redhat.com/errata/RHSA-2004-323.html **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Gentoo: http://security.gentoo.org/glsa/glsa-200409-13.xml** We are not aware of any exploits for this vulnerability.	LHA Multiple Code Execution CVE Names: CAN-2004-0694, CAN-2004-0745, CAN-2004-0769, CAN-2004-0771	High	SecurityFocus, September 2, 2004 **Fedora Update Notifications FEDORA-2004-294 & 295, September 8, 2004** Gentoo Linux Security Advisory, GLSA 200409-13, September 8,2 004
Multiple Vendors Apple Mac OS X 10.2.8, 10.3.4, 10.3.5, Mac OS X Server 10.2.8, 10.3.4, 10.3.5; OpenLDAP OpenLDAP 1.0-1.0.3, 1.1-1.1.4, 1.2-1.2.13, 2.0-2.0.23, 2.0.25, 2.0.27, 2.1 .20, 2.1.4, 2.1.10-2.1.19	A vulnerability exists in the 'userPassword' attribute because a CRYPT password can be used as a plaintext password, which could let a malicious user obtain unauthorized access. Patches available at: http://www.apple.com/support/downloads/ There is no exploit code required.	OpenLDAP CRYPT Password Unauthorized Access CVE Name: CAN-2004-0823	Medium	Apple Security Advisory, APPLE-SA-0024-09-07, September 7, 2004
Multiple Vendors Apache Software Foundation Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.50; Avaya Converged	A remote Denial of Service vulnerability exists in Apache mod_ssl during SSL connections. Apache: http://nagoya.apache.org/bugzilla/show_bug.cgi?id=29964 Avaya: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selected	Apache mod_ssl Remote Denial of Service CVE Name: CAN-2004-0748	Low	SecurityFocus, September 7, 2004

Communications Server 2.0, Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0	Bucket=126655&temp. feedbackState=askForFeedback&temp.documentID=202020&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() RedHat: http://rhn.redhat.com/errata/RHSA-2004-349.html SuSE: ftp://ftp.suse.com/pub/suse/ We are not aware of any exploits for this vulnerability.			
Multiple Vendors FileZilla Server 0.7, 0.7.1; OpenBSD -current, 3.5; OpenPKG Current, 2.0, 2.1; zlib 1.2.1	A remote Denial of Service vulnerability during the decompression process due to a failure to handle malformed input. Gentoo: http://security.gentoo.org/glsa/glsa-200408-26.xml FileZilla: http://sourceforge.net/project/showfiles.php?group_id=21558 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/017_libz.patch OpenPKG: ftp ftp.openpkg.org Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **SuSE: ftp://ftp.suse.com/pub/suse/** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **Conectiva: ftp://atualizacoes.conectiva.com.br/** We are not aware of any exploits for this vulnerability.	Zlib Compression Library Remote Denial of Service CVE Name: CAN-2004-0797	Low	SecurityFocus, August 25, 2004 SUSE Security Announcement, SUSE-SA:2004:029, September 2, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:090, September 8, 2004** **Conectiva Linux Security Announcement, CLA-2004:865, September 13, 2004**
Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3; MandrakeSoft Linux Mandrake 9.2 amd64, 9.2, 10.0 AMD64, 10.0	A vulnerability exists due to insufficient validation of ownership of temporary directories, which could let a malicious user cause a Denial of Service, overwrite arbitrary files, or obtain elevated privileges. KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.0.5b-kdelibs-kstandarddirs.patch Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora:http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required.	KDE Insecure Temporary Directory Symlink CVE Name: CAN-2004-0689	Low/Medium (Low if a DoS)	KDE Security Advisory,August 11, 2004 **Fedora Update Notifications, FEDORA-2004-290 & 291, September 8, 2004** **Conectiva Linux Security Announcement, CLA-2004:864, September 13, 2004**
Multiple Vendors Enlightenment Imlib2 1.0-1.0.5, 1.1, 1.1.1; ImageMagick ImageMagick 5.4.3, 5.4.4 .5, 5.4.8 .2-1.1.0 , 5.5.3 .2-1.2.0, 5.5.6 .0-2003040, 5.5.7,6.0.2; Imlib Imlib 1.9-1.9.14	Multiple buffer overflow vulnerabilities exist in the Iimlib/Imlib2 libraries when handling malformed bitmap images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Imlib: http://cvs.sourceforge.net/viewcvs.py/enlightenment/e17/ ImageMagick: http://www.imagemagick.org/www/download.html **Gentoo: http://security.gentoo.org/glsa/glsa-200409-12.xml** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** We are not aware of any exploits for this vulnerability.	IMLib/IMLib2 Multiple BMP Image Decoding Buffer Overflows CVE Names: CAN-2004-0817, CAN-2004-0802	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 1, 2004 **Gentoo Linux Security Advisory, GLSA 200409-12, September 8, 2004** **Mandrakelinux Security Update Advisory, MDKSA-2004:089, September 8, 2004** **Fedora Update Notifications, FEDORA-2004-300 &301, September 9, 2004**
Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.2-3.2.3; MandrakeSoft Linux Mandrake 9.2 amd64, 9.2, 10.0 AMD64, 10.0	A vulnerability exists in DCOPServer due to insecure file creation, which could let a malicious user obtain elevated privileges or overwrite arbitrary files. KDE: ftp://ftp.kde.org/pub/kde/security_patches/post-3.2.3-kdelibs-dcopserver.patch Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva: ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	KDE DCOPServer Insecure Temporary File Creation CVE Name: CAN-2004-0690	Medium	KDE Security Advisory,August 11, 2004 **Conectiva Linux Security Announcement, CLA-2004:864, September 13, 2004** **US-CERT Vulnerability Note VU#330638, September 7, 2004**
Multiple Vendors Gentoo Linux 1.4; KDE KDE 3.1.3, 3.2, 3.0-3.0.3, 3.0.5b, 3.0.5, 3.1-3.1.3, 3.1.5, 3.2.1, 3.2.3; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64	A vulnerability exists while validating cookie domains, which could let a remote malicious user hijack a target user's session. KDE: ftp://ftp.kde.org/pub/kde/security_patches Gentoo: http://security.gentoo.org/glsa/glsa-200408-23.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Fedora:http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required.	KDE Konqueror Cookie Domain Validation CVE Name: CAN-2004-0746	Medium	KDE Security Advisory, August 23, 2004 **Fedora Update Notifications, FEDORA-2004-290 & 291, September 8, 2004** **Conectiva Linux Security Announcement, CLA-2004:864, September 13, 2004**
Multiple Vendors KDE 3.2.3 and prior	A frame injection vulnerability exists in the Konqueror web browser that allows websites to load web pages into a frame of any other frame-based web page that the user may have open. A malicious website could abuse Konqueror to insert its own frames into the page of an otherwise trusted website. As a result, the user may unknowingly send confidential information intended for the trusted website to the malicious website. Source code patches have been made available which fix these vulnerabilities. Refer to advisory: http://www.kde.org/info/security/advisory-20040811-3.txt Gentoo: http://security.gentoo.org/glsa/glsa-200408-13.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva: ftp://atualizacoes.conectiva.com.br/**	Konqueror Frame Injection Vulnerability CVE Name: CAN-2004-0721	Low	KDE Security Advisory 20040811-3, August 11, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:086, August 21, 2004 **Fedora Update Notifications, FEDORA-2004-290 & 291, September 8, 2004**

	Fedora:http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ A Proof of Concept exploit has been published.			**Conectiva Linux Security Announcement, CLA-2004:864, September 13, 2004**
Multiple Vendors Linux Kernel 2.4.27	A Denial of Service vulnerability exists when processing TCP sockets. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Linux Kernel TCP Socket Denial of Service	Low	SecurityTracker Alert ID, 1011245, September 14, 2004
Multiple Vendors Luke Mewburn lukemftp 1.5, TNFTPD 20031217; NetBSD Current, 1.3-1.3.3, 1.4 x86, 1.4, SPARC, arm32, Alpha, 1.4.1 x86, 1.4.1, SPARC, sh3, arm32, Alpha, 1.4.2 x86, 1,4.2, SPARC, arm32, Alpha, 1.4.3, 1.5 x86, 1.5, sh3, 1.5.1-1.5.3, 1.6, beta, 1.6-1.6.2, 2.0	Several vulnerabilities exist in the out-of-band signal handling code due to race condition errors, which could let a remote malicious user obtain superuser privileges. Luke Mewburn Upgrade: ftp://ftp.netbsd.org/pub/NetBSD/misc/tnftp/tnftpd-20040810.tar.gz **Apple: http://wsidecar.apple.com/cgi-bin/** We are not aware of any exploits for this vulnerability.	TNFTPD Multiple Signal Handler Remote Privilege Escalation CVE Name: CAN-2004-0794	High	NetBSD Security Advisory 2004-009, August 17, 2004 **Apple Security Update, APPLE-SA-2004-09-07, September 7, 2004**
MySQL AB MySQL 3.23.49, 4.0.20	A vulnerability exists in the 'mysqlhotcopy' script due to predictable files names of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/m/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-02.xml **SuSE: ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	MySQL 'Mysqlhotcopy' Script Elevated Privileges CVE Name: CAN-2004-0457	Medium	Debian Security Advisory, DSA 540-1, August 18, 2004 Gentoo Linux Security Advisory GLSA 200409-02, September 1, 2004 **SUSE Security Announcement, SUSE-SA:2004:030, September 6, 2004**
OpenOffice OpenOffice 1.1.2, Sun StarOffice 7.0	A vulnerability exists in the '/tmp' folder due to insecure permissions, which could let a malicious user obtain sensitive information. Upgrades available at: http://sunsolve.sun.com/search/ There is no exploit code required.	OpenOffice/ StarOffice Insure Temporary File Permissions	Medium	Secunia Advisory, SA12302, September 13, 2004
Paul LDaniels ripMIME prior to 1.4.0.0	Multiple vulnerabilities exist: a vulnerability exists because a remote malicious user can submit MIME content that contains certain fields that occur multiple times to bypass filtering functions; a vulnerability exists because a remote malicious user can use malformed MIME encapsulation techniques that use non-standard separators (such as a double colon) to bypass content filtering functions; a vulnerability exists because a remote malicious user can use malformed MIME encapsulation techniques that include fields encoded using the RFC 2231 continuations or parameter value character set and language information to bypass content filtering functions; and a vulnerability exists because a remote malicious user can use malformed MIME encapsulation techniques that include fields containing an RFC 822 comment to bypass content filtering functions. Updates available at: http://www.pldaniels.com/ripmime/downloads.php We are not aware of any exploits for this vulnerability.	ripMIME MIME Decoding Multiple Vulnerabilities CVE Names: CAN-2003-1014, CAN-2004-0052, CAN-2004-0161, CAN-2004-0162	Medium	Corsaire Security Advisory, September 13, 2004
PHPGroupWare PHPGroupWare 0.9.12, 0.9.13, 0.9.14 .003, 0.9.14.005-0.9.14.007, 0.9.16 RC1, 0.9.16 .002, 0.9.16 .000	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://downloads.phpgroupware.org/files/0.9.16-release/phpgroupware-0.9.16.003.tar.gz There is no exploit code required.	PHPGroupWare Wiki Cross-Site Scripting	High	Secunia Advisory, SA12466, September 6, 2004
rsync 2.6.2 and prior Debian SuSE Trustix	A vulnerability exists in rsync when running in daemon mode with chroot disabled. A remote user may be able read or write files on the target system that are located outside of the module's path. A remote user can supply a specially crafted path to cause the path cleaning function to generate an absolute filename instead of a relative one. The flaw resides in the sanitize_path() function. Updates and patches are available at: http://rsync.samba.org/ SuSE: http://www.suse.de/de/security/2004_26_rsync.html Debian: http://www.debian.org/security/2004/dsa-538 Trustix: http://www.trustix.net/errata/2004/0042/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-17.xml Netwosix: http://www.netwosix.org/adv17.html Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/rsync-2.6.0-2.0.2.src.rpm Tinysofa: http://http.tinysofa.org/pub/tinysofa/updates/server-2.0/i386/tinysofa/rpms.updates/rsync-2.6.2-2ts.i386.rpm TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-436.html** We are not aware of any exploits for this vulnerability.	Rsync Input Validation Error in sanitize_ path() May Let Remote Users Read or Write Arbitrary Files	High	SecurityTracker 1010940, August 12, 2004 rsync August 2004 Security Advisory OpenPKG Security Advisory, OpenPKG-SA-2004.037, August 15, 2004 Tinysofa Security Advisory, TSSA-2004-020-ES, August 16, 2004 Gentoo Linux Security Advisory GLSA 200408-17, August 17, 2004 Netwosix Linux Security Advisory, LNSA-#2004-0017, August 17, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:083, August 17, 2004 Fedora Update Notification, FEDORA-2004-269, August 19, 2004 Turbolinux Security Advisory, TLSA-2004-20, August 31, 2004 **RedHat Security Advisory, RHSA-2004:436-07,**

				September 1, 2004
SAFE TEAM Regulus 2.2 -95	Several vulnerabilities exist: a vulnerability exists in the 'staffile' file, which could let a remote malicious user obtain sensitive information; a vulnerability exists because a specified user/customer password hash is contained in a hidden tag of the 'Update Your Password' action page; and a vulnerability exists because it is possible to view a target users connection statistics without requiring valid credentials. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	SAFE TEAM Regulus Information Disclosure	Medium	SecurityFocus, September 7, 2004
Samba.org Samba 2.2.11, 3.0.6	A remote Denial of Service vulnerability exists due to the way print change notify requests are processed. Trustix: http://http.trustix.org/pub/trustix/updates/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-14.xml** We are not aware of any exploits for this vulnerability.	Samba Remote Print Change Notify Remote Denial of Service	Low	Trustix Secure Linux Security Advisory, TSL-2004-0043, August 26, 2004 **Gentoo Linux Security Advisory [ERRATA UPDATE] GLSA 200409-14:02, September 9, 2004**
Samba.org Samba version 3.0 - 3.0.6	Several vulnerabilities exist: a remote Denial of Service vulnerability exists in the 'process_logon_packet()' function due to insufficient validation of 'SAM_UAS_CHANGE' request packets; and a remote Denial of Service vulnerability exists when a malicious user submits a malformed packet to a target 'smbd' server. Updates available at: http://samba.org/samba/download/ We are not aware of any exploits for this vulnerability.	Samba Remote Denials of Service CVE Names: CAN-2004-0807, CAN-2004-0808	Low	Securiteam, September 14, 2004
Squid-cache.org Squid 2.5.STABLE6 & prior	A remote Denial of Service vulnerability exists due to a buffer overflow in the 'clientAbortBody()' function in 'client_side.c.' No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Squid 'clientAbortBody()' Remote Denial of Service	Low	SecurityTracker Alert ID, 1011214, September 11, 2004

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
BEA Systems WebLogic Server & Express 7.0, 8.1	A vulnerability exists in the JNDI tree due to insufficient protection of internal server objects, which could let a remote malicious user obtain sensitive information. Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-65.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic Information Disclosure	Medium	BEA Security Advisory, BEA04-65.00, September 13, 2004
BEA Systems WebLogic Server & Express 6.1 SP6, 7.0 SP4, 8.1 SP2; and prior service packs	A vulnerability exists because some scripts used to run command line utilities and Administrative ant tasks may contain clear-text passwords, which could let a malicious user obtain sensitive information. Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-68.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic Command & Administrative Scripts Password Disclosure	Medium	BEA Security Advisory, BEA04-68.00, September 13, 2004
BEA Systems WebLogic Server & Express 6.1 SP6, 7.0 SP5, 8.1 SP2; and prior service packs	A vulnerability exists because some URL patterns in the 'web.xml' file may not be processed properly when running on operating systems that have case-sensitive filenames, which could let a remote malicious user obtain unauthorized access to restricted URLs. Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-67.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic Case-Sensitive 'web.xml' Patterns	Medium	BEA Security Advisory, BEA04-67.00, September 13, 2004
BEA Systems WebLogic Server & Express 6.1 SP6, 7.0 SP5, 8.1 SP3; and prior service packs	A vulnerability exists because by default server version information is disclosed in response to HTTP and HTTPS requests, which could let a remote malicious user obtain sensitive information. Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-70.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic System Version Information Disclosure	Medium	BEA Security Advisory, BEA04-70.00, September 13, 2004
BEA Systems WebLogic Server & Express 7.0 SP5, 8.1 SP2; and prior	A vulnerability exists because a remote malicious user with RMI access to the administration server can execute some 'weblogic.Admin' commands, which could lead to the disclosure of sensitive information or the execution of arbitrary code. Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-66.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic 'weblogic.Admin' commands	Medium/ High (High if arbitrary code can be executed)	BEA Security Advisory, BEA04-66.00, September 13, 2004
BEA Systems WebLogic Server & Express 7.0 SP5, 8.1 SP2; and prior service packs	A vulnerability exists when using an Active Directory LDAP server as the authentication database due to insufficient restrictions of disabled users, which could let a remote authenticated malicious user obtain access to their disabled account. Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-72.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic Active Directory LDAP Disabled User's Accounts	Medium	BEA Security Advisory, BEA04-72.00, September 13, 2004
BEA Systems WebLogic Server & Express 7.0 SP5, 8.1 SP2; and prior service packs	A vulnerability exists during deployment when an internal error occurs, which could lead to the deployment of the application with 'incomplete security.' Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-71.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic Server Incomplete Security Deployment	Medium	BEA Security Advisory, BEA04-71.00, September 13, 2004
BEA Systems WebLogic Server & Express 7.0, 8.1	A vulnerability exists when the administration port is not enabled because sensitive data and configuration information is transmitted in clear text, which could let a remote malicious user obtain sensitive information. Fixes available at: dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04-73.00.jsp We are not aware of any exploits for this vulnerability.	WebLogic Clear Text Sensitive Information Transmit	Medium	BEA Security Advisory, BEA04-73.00, September 13, 2004
eZ Systems eZ 3.4, eZphotoshare 1.0, 1.1, 1.2.1	A remote Denial of Service vulnerability exists due to a connection handling error. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	eZ/eZphotoshare Remote Denial of Service	Low	SecurityFocus, September 7, 2004
FocalMedia.Net Turbo Seek 1.x	A vulnerability exists in 'tseekdir.cgi' because input passed to the 'location' variable is not handled correctly, which could let a remote malicious user obtain sensitive information. Update available at: http://www.focalmedia.net/tbdownload.html	Turbo Seek Information Disclosure	Medium	LwB Security Team Advisory # 17, September 10, 2004

	Proofs of Concept exploits have been published.			
Gearbox Software Halo Combat Evolved 1.2, 1.4, 1.31	A remote Denial of Service vulnerability exists due to an off-by-one error in the handling of client connections. MacSoft Upgrade available at: http://files.bungie.org/halo105_updater.sit Microsoft Upgrade available at: http://download.microsoft.com/download/2/d/2/2d2d17f1-7436-46a5-a9c7-c15909cd673f/halopc105.exe An exploit script has been published.	Halo Combat Evolved Game Server Remote Denial of Service	Low	Bugtraq, September 9, 2004
Lexar Lexar JumpDrive Secure USB Flash Drive 1.x	A vulnerability exists because a local malicious user can read the encrypted password. We are not aware of any exploits for this vulnerability. No workaround or patch available at time of publishing.	Lexar JumpDrive Password Disclosure	Medium	Secunia Advisory, SA12522, September 14, 2004
NTSOFT BBS E-Market Professional	Multiple vulnerabilities exist: a vulnerability exists in the 'becommunity' script due to insufficient verification of input passed to the 'pageurl' parameter, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in 'index.php' when an invalid value is submitted to the 'from_market' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	BBS e-Market Professional Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID: 1011204, Security Tracker, September 10, 2004
Pingtel Corp. Model PX-1, Core Apps firmware 2.1.11.24, Kernel firmware 2.1.11.24	A remote Denial of Service vulnerability exists in the HTTP management interface of the phone when a malicious user submits a specially crafted request. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Pingtel xpressa Remote Denial of Service	Low	@stake, Inc. Security Advisory, September 13, 2004
PostNuke Modules Factory Subjects Module 2.0	An input validation vulnerability exists in the 'subid,' 'pageid,' and 'catid' parameters due to insufficient sanitization before being used in SQL queries, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PostNuke Modules Factory Subjects Module Input Validation	High	CRIOLABS Security Advisory, September 9, 2004
psnews.sourceforge.net PSnews 1.1	A Cross-Site Scripting vulnerability exists due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploit scripts have been published.	PSnews Cross-Site Scripting	High	SecurityTracker Alert ID: 1011191, September 8, 2004
QNX Software Systems Ltd. QNX RTP 6.1	A vulnerability exists in the 'crrtrap' application, which could let a malicious user obtain root access. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	QNX crrtrap Race Condition	High	rfdslabs Security Advisory, RLSA_04-2004, September 13, 2004
QNX Software Systems Ltd. QNX RTP 6.1	Several buffer overflow vulnerabilities exist in the '-s' (server) flag, which could let a malicious user obtain root access. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	QNX Binaries Buffer Overflows in '-s' Switch	High	rfdslabs Security Advisory, RLSA_04-2004, September 13, 2004
Ulrik Petersen Emdros Database Engine 1.1.14-1.1.19	A remote Denial of Service vulnerability exists in the 'CFeatureDeclaration::TypeTypeCompatibility()' function due to a memory leak. Upgrade available at: http://prdownloads.sourceforge.net/emdros/emdros-1.1.20.tar.gz?download There is no exploit code required.	Emdros Remote Denial of Service	Low	Secunia Advisory, SA12486, September 8, 2004
UtilMind Solutions Site News 1.1	An authentication bypass vulnerability exists due to an access validation error, which could let a malicious user manipulate information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Site News Authentication Bypass	Medium	SecurityTracker Alert ID, 1011159, September 5, 2004

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
September 14, 2004	5YP0B15E0S.html	Yes	Proof of concept exploit for the cdrecord configuration vulnerability that a local user can exploit to obtain root privileges.
September 14, 2004	adv17.txt	Yes	Proof of concept exploit for Turbo Seek 1.x vulnerability that allows an attacker the ability to access the contents of any file in the file system.
September 14, 2004	rkhunter-1.1.8.tar.gz	N/A	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
September 13, 2004	portknock-sshd_lkm.c	N/A	Kernel module using portknocking to get sshd spawned after challenging a list of specified daemons. Designed for 2.4 kernels.
September 13, 2004	readcd_exp.sh	Yes	Local root exploit for readcd that comes setuid default on some Linux distributions.
September 13, 2004	sm00ny-courier_imap_fsx.c	Yes	Exploit for courier-imap 3.0.2-r1 and below remote format string vulnerability.
September 10, 2004	adv06-y3dips-2004.txt	No	Proof of concept exploit for the 1n BBS E-Market Professional remote command execution vulnerabilities via remote file inclusion and full path disclosure flaw.
September 10, 2004	BJDExploit.rar	Yes	Buffer overflow exploit for BlackJumboDog FTP server version 3.6.1 that opens up port 7777 allowing for an executable upload.
September 10, 2004	BlackJumboDog_ftp_exp.c	Yes	Proof of concept exploit for the buffer overflow vulnerability in SapporoWorks Black JumboDog FTP Server 3.6.1
September 10, 2004	cdr_exp.sh	Yes	Local root exploit for cdrecord, which fails to drop euid=0 when it exec()s a program specified by the user through the RSH environment variable.
September 10, 2004	fed.ipSpace.txt	N/A	A list of IP space for various Federal agencies.
September 10, 2004	haloboom.zip	Yes	Proof of concept Denial of Service exploit for Halo: Combat Evolved versions 1.4 and below which suffer from an off-by-one vulnerability.
September 10, 2004	None	No	Proof of concept exploit for GetSolutions GetIntranet SQL injection vulnerabilities.
September 10, 2004	None	No	Proof of concept exploit for GetSolutions GetInternet SQL injection vulnerabilities.
September 10, 2004	osxrk-0.2.1.tbz	N/A	MAC OS-X rootkit that has a lot of standard tools included, adds a TCP backdoor via inetd, does data recon, and more.

September 10, 2004	phpSQLnuke.pl	Yes	Perl exploit that makes use of a flaw in PHP-Nuke 7.4 where an attacker can post to global home-page messages.
September 10, 2004	subjects2.txt	No	Proof of concept exploit for the PostNuke Subjects module 2.x SQL injection attack vulnerability.
September 10, 2004	trillian074i.txt	No	Proof of concept exploit for the buffer overflow vulnerability in the Trillian basic edition version 0.74i. This vulnerability is remotely exploitable but requires the use of a man-in-the-middle attack.
September 10, 2004	weplab-0.1.1-beta.tar.gz	N/A	Weplab is a tool to review the security of WEP encryption in wireless networks from an educational point of view.
September 9, 2004	aircrack-2.0.tgz	N/A	Aircrack is an 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered.
September 9, 2004	codboom.zip	Yes	Proof of concept exploit for Call of Duty versions 1.4 and below Denial of Service vulnerability.
September 9, 2004	drizzit.c	Yes	Proof of concept exploit for the AIM Away Message buffer overflow vulnerability. Affects AIM versions 5.5.3588, 5.5.3590 Beta, 5.5.3591, 5.5.3595 and others.
September 9, 2004	dynalink.Backdoor.txt	No	Proof of concept exploit for the Dynalink RTA 230 ADSL router backdoor account vulnerability.
September 9, 2004	elf-0.5.4p1.tar.gz	N/A	A command-line tool that allows a user to analyze the contents of an ELF object file header. This header contains various integral values such as the virtual entry point of the object file, the machine architecture it was compiled for and more.
September 9, 2004	exploits-1.tbz	N/A	A collection of tutorials regarding exploit programming.
September 9, 2004	MailWorks.txt	Yes	Proof of concept exploit for the MailWorks Pro session check bypass vulnerability. The exploit allows an attacker to have full control over the administration section.
September 9, 2004	neb-private.c	Yes	Proof of concept exploit for the Citadel/UX versions 6.23 and below USER directive overflow vulnerability.
September 9, 2004	qnx-pppoed-multiple-flaws.txt	No	Proof of concept for the QNX PPPoEd multiple local root vulnerabilities. QNX RTP 6.1 is affected.
September 9, 2004	sitenewsAuth.txt	No	Proof of concept exploit for the Site News 1.1 authentication vulnerability.
September 9, 2004	torrent_exp.php.txt	Yes	Proof of concept PHP exploit that makes use of a SQL injection vulnerability in TorrentTrader version 1.0 RC2.
September 8, 2004	Trillian_bof.c	No	Script that exploits the Trillian Remote Buffer Overflow MSN Module vulnerability.
September 7, 2004	cdrdaohack.sh cdrdao_show_file.sh cdrdao-exp.sh	No	Exploits for the CDRDAO configuration vulnerability which could result in the overwriting of root-owned files, or potentially allow the user execute commands as root.
September 7, 2004	None	No	Proof of concept exploit for UtilMind Solutions Site News authentication bypass vulnerability.
September 7, 2004	None	No	Proof of concept exploit for the input verification vulnerability in PSnews.
September 7, 2004	typsoft_ftpd_dos.bat	No	Proof of Concept exploit script for the TYPSoft FTP Server Remote 'RETR' Command Denial of Service vulnerability.
September 6, 2004	codboom.zip	Yes	Proof of concept exploit for Call of Duty input validation vulnerability.
September 4, 2004	wottapoop.html	Yes	Proof of concept exploit for the Microsoft Internet Explorer drag and drop installation vulnerability.

[back to top]

Trends

- The number of inappropriate or offensive images sent as attachments in the past six months was dramatically lower than the same period last year, according to MessageLabs, a U.K.-based managed message security service. Also in August, MessageLabs spotted a decline in both spam and virus-laden e-mails. During August, MessageLabs tagged 84.2 percent of all messages it scanned as spam, down from July's 94.6 percent. Virus-contaminated mail also fell in August to 6.9 percent of the scanned messages; during July, MessageLabs found malicious code in 7.3 percent of the mail it processed. Possible explanations for the declines include a growing enforcement of corporate governance requirements, the cyclical nature of virus outbreaks with summer months tending to be calm, and the United States' Operation Web Snare conducted in August during which more than 150 people were arrested for a variety of online criminal activities, including spamming. (Source: InternetWeek.com, September 7, 2004)
- Phishing is reaching epidemic proportions. The Anti-Phishing Working Group (APWG), a vendor consortium trying to address the problem, received reports of more than 1,100 unique phishing campaigns in April, a 178 percent increase from the previous month and a 4,000 percent increase from November 2003. A Gartner Group study, also completed in April, estimated that more than 57 million Americans, representing 40 percent of all online users, received a phishing e-mail, and 76 percent said the attack had taken place in the last six months.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Increase	March 2004
5	Netsky-B	Win32 Worm	Stable	February 2004
6	Mydoom.q	Win32 Worm	Decrease	August 2004
7	Bagle-AA	Win32 Worm	Slight Increase	April 2004
8	MyDoom-O	Win32 Worm	Slight Increase	July 2004
9	Netsky-Q	Win32 Worm	Slight Increase	March 2004
10	Mydoom.m	Win32 Worm	Decrease	July 2004

Top Ten Table updated September 10, 2004

Viruses or Trojans Considered to be a High Level of Threat

- **Amus:** While not a severe threat, the Amus worm is one of the more unique worms to have surfaced. The worm spreads via Outlook to e-mails found in the Windows Address Book, and if the attachment is executed by the user, the worm generates a short message in a robotic female voice, using Windows XP's built-in speech capabilities. The worm may also attempt to delete all INI or DLL files from the Windows folder.
- **Sdbot:** Anti-virus companies are warning of a new variant of the Sdbot mass-mailing worm that installs a network sniffer in order to grab unencrypted passwords, apparently the first worm to do so. The worm creates a bot that uses functions of NetBEUI (NetBios Extended User Interface), a protocol used by network operating systems, to find usernames and passwords, and uses these to create copies of itself on shared folders.

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
AdClicker-AZ		Redirect Code
Amus	Amus.a I-Worm.Amus.a W32/Amus.a@MM W32/Amus-A	Win32 Worm

Backdoor.IRC.Lazz		Trojan
Backdoor.Nemog.B		Trojan
Backdoor.Nemog.C		Trojan
BackDoor-CEB.c	Backdoor.Nemog.B Backdoor.Win32.Surila.i Win32.Gavvo.C	Trojan
BackDoor-CIL		Trojan
BackDoor-CIO		Trojan
Bizex.E	Trojan/Bizex-E TrojanSpy.Win32.Small.az	Trojan
Downloader-OE		Trojan
Downloader-OO		Trojan
Downloader-PG		Trojan
Linux/BackDoor-Rooted		Linux Trojan
Mydoom.T	W32.Mydoom.T@mm	Win32 Worm
Mydoom.U	I-Worm.Mydoom.s MyDoom.U W32.Mydoom.S@mm W32.Mydoom.U@mm W32/MyDoom-U W32/Mydoom.U.worm W32/Mydoom.U@mm Win32.Mydoom.U Win32/Mydoom.Variant.Worm	Win32 Worm
Mydoom.V	I-Worm.Mydoom.t W32/Mydoom.V.worm W32.Mydoom.V@mm	Win32 Worm
Mydoom.W	I-Worm.Mydoom.t W32/Mydoom.W.worm	Win32 Worm
Mydoom.X	I-Worm.Mydoom.p I-Worm.Mydoom.v W32.Mydoom.gen@mm W32/Mydoom.r@MM W32/Mydoom.X.worm W32/Mydoom.X@mm Win32.Mydoom.X Win32/Mydoom.Variant.Worm	Win32 Worm
Mydoom.Y	I-Worm.Mydoom.v W32.Mydoom.V@mm Win32.Mydoom.Y Win32/Mydoom.Variant.Worm ZIP.Mydoom.Y	Win32 Worm
Mydoom.z	W32/Mydoom.z@MM	Win32 Worm
MyDoom-W	W32/MyDoom-W W32.Mydoom.W@mm	Win32 Worm
ProcKill-BX		Trojan
Proxy-Speednet		Proxy Virus
PWSteal.Bancos.L		Password Stealer
PWSteal.Eyoni		Trojan: Password Stealer
Sdbot.AQA	W32/Sdbot.AQA.worm	Win32 Worm
Troj/Optix-PRO	Backdoor.OptixPro.13 Backdoor.Optix.b BackDoor-ACH trojan Win32/Optix.Pro.131 trojan	Win32 Worm
Troj/Psyme-AS		Trojan
Trojan.Dasda		Trojan
Trojan.Kreol		Trojan
Trojan.Riler		Trojan
TrojanDownloader.JS.Gen		Trojan
Uploader-S	TR/small.az3	Trojan
W32.Gaobot.BIA		Win32 Worm
W32.Gaobot.BIE		Win32 Worm
W32.Gaobot.BIQ		Win32 Worm
W32.IRCBot.G		Trojan
W32.IRCBot.H		Win32 Worm
W32.Mydoom.S@mm		Win32 Worm
W32.Spybot.DHV		Win32 Worm
W32.Spybot.DNB		Win32 Worm
W32.Spybot.DNC		Win32 Worm
W32.Sykel	W32.Multex.B Win32/HLLW.Secef.A Worm.P2P.Multex.b	Win32 Worm
W32/Alizado.worm		Win32 Worm
W32/Bagle-AM		Win32 Worm
W32/Forbot-Q	W32/Gaobot.worm.gen.g1 Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-V	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/MyDoom-V	W32/Mydoom.v@MM I-Worm.Mydoom-t WORM_MYDOOM.GEN	Win32 Worm
W32/MyDoom-X		Win32 Worm
W32/Nyxem-C	W32/MyWife.c@MM I-Worm.Nyxem.d	Win32 Worm
W32/Rbot-IK	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-IL	WORM_RBOT.OA	Win32 Worm
W32/Rbot-IO	Backdoor.Rbot.gen W32/Sdbot.worm.gen.t virus	Win32 Worm
W32/Rbot-IT	W32/Sdbot.worm.gen.i Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-IY		Win32 Worm
W32/Rbot-JC	Backdoor.Rbot.gen	Win32 Worm

	W32.Spybot.Worm WORM_RBOT.CX	
W32/Sdbot-OV	W32/Sdbot.worm.gen.h WORM_RANDEX.L Backdoor.Win32.SdBot.ry	Win32 Worm
W32/Sdbot-OY	W32/Sdbot.worm.gen.h1 WORM.SDBOT.QR Backdoor.SdBot.gen	Win32 Worm
W32/Sdbot-RY	W32/Sdbot.worm.gen.h Backdoor.Win32.SdBot.ry	Win32 Worm
Win32.Cissi.H	W32/Imbiat.worm Win32/Pinom.C.Worm Worm.Win32.Pinom.c	Win32 Worm
Win32.Dluca.J	Downloader-DC Win32/Dluca.J.Trojan	Win32 Worm
Win32.Lovgate.BD	I-Worm.LovGate.ah W32.Lovgate.Gen@mm W32/Lovgate.an@MM Win32.Lovgate.BD Win32/LovGate.AZ.Worm	Win32 Worm
Win32.Randin.A	Win32/Randin.A.Worm Worm.Win32.Randin.a	Win32 Worm
Win32.Wintrim.U		Win32 Worm
WitchDoc		Trojan
Wootbot	Backdoor.Win32.Wootbot Backdoor.Win32.Wootbot.gen Backdoor.Wootbot Backdoor.Wootbot.gen	Trojan
WORM_BLUEWORM.D	I-Worm.Nyxem.c W32/Mywife.D.worm	Win32 Worm
WORM_BLUEWORM.F	I-Worm.Nyxem.d W32.Blackmal.C@mm W32/Mywife.C.worm W32/MyWife.c@MM W32/Nyxem-C	Win32 Worm
Zusha	Trojan.Win32.Small.aq TrojanDownloader.Win32.Agent.co W32.HLLW.Zusha Worm.Win32.Zusha.a Worm.Win32.Zusha.b	Win32 Worm

[back to top]

Last updated September 15, 2004